(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 48 767 A1**

(51) Int. Cl.[6]:
G 07 C 9/00
G 07 F 7/10
G 06 K 19/07
A 61 B 5/117

(21) Aktenzeichen: 196 48 767.6
(22) Anmeldetag: 25. 11. 96
(43) Offenlegungstag: 26. 6. 97

DE 196 48 767 A1

(30) Unionspriorität: (32) (33) (31)
21.12.95 AT 2084/95

(71) Anmelder:
Siemens AG Österreich, Wien, AT

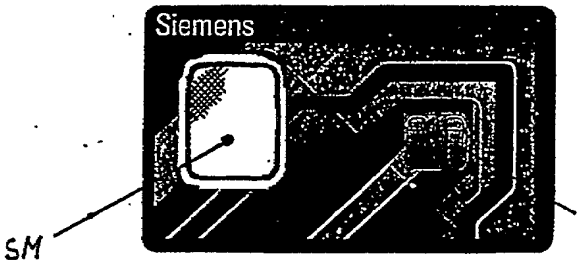
(74) Vertreter:
Fuchs, F., Dr.-Ing., Pat.-Anw., 81541 München

(72) Erfinder:
Rechberger, Rudolf, Steinriegl, AT

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Identifikationssystem mit elektronischer Chipkarte

(57) Es wird ein Identifikationssystem mit elektronischer Chipkarte, mit Speichern (VSL) für biometrische Identifikationsmerkmale der benutzungsberechtigten Personen, mit Sensoren (SM) zum Erfassen der biometrischen Identifikationsmerkmale und Mitteln (VSL) zum Vergleich der gespeicherten und der erfaßten biometrischen Identifikationsmerkmale angegeben, bei dem die Mittel zum Speichern, zur Erfassung und zum Vergleich der biometrischen Identifikationsmerkmale jeweils zumindest teilweise in der Weise in die Chipkarte integriert sind, daß ein autonomer Vergleich der gespeicherten mit den erfaßten biometrischen Identifikationsmerkmale möglich ist.
Damit ist eindeutige und manipulationssichere Personenidentifizierung ohne PIN-Nummer oder Foto möglich.



DE 196 48 767 A1

Beschreibung

Die Erfindung betrifft ein Identifikationssystem mit elektronischer Chipkarte, mit Speichern für biometrische Identifikationsmerkmale der benutzungsberechtigten Personen, mit Sensoren zum Erfassen der biometrischen Identifikationsmerkmale und Mitteln zum Vergleich der gespeicherten und der erfaßten biometrischen Identifikationsmerkmale.

Die Verbreitung und Vermarktung von Dienstleistungen, bei denen auf geschützte Daten zugegriffen werden muß, erfolgt in zunehmendem Maß mittels Systemen zur elektronischen Datenverarbeitung, wobei elektronische Chipkarten eine wesentliche Rolle spielen. So werden sie beispielsweise bei den sogenannten Geldausgabeautomaten in Verbindung mit einer individuellen Kennung — der PIN-Nummer — zur Berechtigungsüberprüfung verwendet, oder auch als elektronische Geldbörse, auf die Geldbeträge aufgebucht werden können, die dann im bargeldlosen Zahlungsverkehr in Geschäften durch entsprechende Chipkarten-Schreib/Lesegeräte wieder abgebucht werden.

Durch die Kombination von Chipkarte und PIN-Nummer wird zwar die Wahrscheinlichkeit einer mißbräuchlichen Verwendung verringert, gleichzeitig aber auch der Komfort für den Benutzer verringert, die Fehlerhäufigkeit bei den Bedienvorgängen erhöht und der Vorgang der Berechtigungskontrolle verlängert, was beispielsweise in Hauptgeschäftszeiten zu erheblichen Wartezeiten und Warteschlangen vor den Geldausgabeautomaten führt.

Erschwerend wirkt sich dabei auch der vielfältige Einsatz verschiedener Chipkarten für die unterschiedlichsten Services in der Telekommunikation, bei der Zutrittskontrolle zu Hochsicherheitsbereichen wie Rechenzentren, oder im Gesundheitswesen aus, so daß sich der Anwender für den Einsatz der verschiedenen Chipkarten auch unterschiedliche PIN-Nummern merken muß.

Viele Benutzer notieren sich daher die PIN-Nummer und verringern damit die Sicherheit der Kombination Chipkarte-PIN-Nummer ganz beträchtlich.

Insbesondere für Zutrittskontrollen werden daher bereits Systeme angeboten, bei denen auf einer Chipkarte biometrische Daten — beispielsweise ein Fingerabdruck — eines Berechtigten gespeichert werden, die im Anwendungsfall, bei der Zutrittskontrolle von einem Kontrollgerät, meist einem Personalcomputer mit einem angeschlossenen Sensor mit dem Fingerabdruck des Benutzers verglichen werden, und bei Übereinstimmung der beiden Abdruckdaten der Zutritt freigegeben wird.

Aus der WO 94/25938 ist weiterhin ein System zur Fingerprint-Identifikation bekannt, bei dem ein Fingerprint-Sensor in eine Chipkarte integriert ist.

Nachteilig an den genannten Systemen ist insbesondere, daß sicherheitsrelevante Daten — die Information über den Fingerabdruck — von der Chipkarte auf ein Kontrollsystem übertragen werden und damit ausgespäht werden können.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Identifikationssystem anzugeben, das höchsten Sicherheitsanforderungen genügt.

Erfindungsgemäß geschieht dies mit einem Identifikationssystem der eingangs genannten Art, bei dem die Mittel zum Speichern (VSL), zur Erfassung (SM) und zum Vergleich (VSL) der biometrischen Identifikationsmerkmale jeweils zumindest teilweise in der Weise in

die Chipkarte integriert sind, bei dem ein autonomer Vergleich der gespeicherten mit den erfaßten biometrischen Identifikationsmerkmale möglich ist und kein Austausch sicherheitsrelevanter Daten zwischen der elektronischen Chipkarte und den übrigen Komponenten des Identifikationssystemes erfolgt.

Für die Identifikation geeignete personenbezogene Merkmale sind beispielsweise das Muster der Blutbahnen der Netzhaut, die Struktur der Iris, die Länge und Form der Finger, das Gesicht, die Stimme oder aber Fingerabdrücke. Die Möglichkeiten, Personen aufgrund dieser Merkmale zu identifizieren, sind beispielsweise in IEEE Spectrum, Februar 1994, "It had to be you" beschrieben. Die wahrscheinlich am besten erforschten und damit zuverlässigsten Merkmale sind dabei die Fingerabdrücke, wobei durch Überprüfung mehrerer Fingerabdrücke noch die Zuverlässigkeit erhöht werden kann. Diese sind auch in für den Benutzer komfortabler Weise zu ermitteln, während z. B. das Muster der Netzhaut nur durch eine für den zu Identifizierenden unangenehme Prozedur erfaßt werden kann und daher nur in jenen Fällen angewendet werden wird, in denen dieser Effekt keine Rolle spielt oder ggf. sogar erwünscht ist.

Vorteilhaft ist es, wenn die Sensoren zum Erfassen des zumindest einen Fingerabdruckes ein Transistorarray beinhalten, und wenn die Transistoren so geschaltet sind, daß das thermische Abbild des zumindest einen Fingerabdruckes erfaßt wird. Transistoren zeichnen sich bekanntlich durch hohe Integrationsfähigkeit aus, ein derart gestalteter Sensor kann daher mit geringen Abmessungen, insbesondere geringer Dicke hergestellt werden.

Die Erfindung wird anhand von Figuren näher erläutert. Es zeigen beispielhaft:

Fig. 1 eine erfindungsgemäß gestaltete Chipkarte,

Fig. 2 einen Querschnitt durch die Chipkarte nach **Fig.** 1,

Fig. 3 die Handhabung einer Chipkarte nach **Fig.** 1 und **Fig.** 2,

Fig. 4 eine schematische Darstellung des Ablaufes bei der Identifikationsprüfung und

Fig. 5 Aufbau eines Identifikationssystemes, bei dem als biometrisches Identifikationsmerkmal die Netzhaut abgetastet wird.

Kernstück des erfindungsgemäßen Identifikationssystemes ist die Chipkarte nach den **Fig.** 1, 2 und 3. Sie beinhaltet neben einer Speicher- und Vergleichslogik VSL, zwei aus einzelnen Transistoren aufgebaute Sensormatrizen SM, mit denen die Fingerabdrücke von Daumen D und Zeigefingers Z erfaßt werden. Um die Handhabung der Karte zu erleichtern, kann auch auf eine Sensormatrix und die Erfassung des Zeigefingerabdruckes verzichtet werden.

Die Stromversorgung der Chipkarte erfolgt über ein Schreib/Lesegerät SLG zu dem auch eine Datenverbindung besteht, über welche der für den vorgesehenen Anwendungszweck notwendige Datenaustausch erfolgt. Bei Einsatz der Chipkarte als elektronische Geldbörse handelt es sich dabei um Auf- bzw. Abbuchung von elektronischen Geldwerten.

Für den Identifikationsvorgang relevante Daten, wie beispielsweise das gespeicherte Fingerabdruckmuster werden über diese Datenverbindung nicht ausgetauscht, so daß diese Daten auch nicht über entsprechend präparierte Schreib/Lesegeräte ausgespäht werden können.

Die Sensormatrizen SM umfassen ein Raster von Transistoren, die so beschaltet sind, daß sie als Temperaturfühler dienen. Damit werden Hautrillenkuppen

und Hautrillensenken bei Anlegen eines Fingers auf die Sensormatrix über die Temperaturunterschiede erfaßt.

Anhand der **Fig.** 4 wird der Ablauf eines Identifikationsvorganges erläutert:

Bei dem Ausführungsbeispiel wird der Fingerabdruck in eine bestimmte Zahl von signifikanten Teilabdrücken zerlegt. Jeder Identifikationsvorgang bedient sich lediglich eines Teils der Teilabdrücke die zufällig oder pseudozufällig ausgewählt werden. Diese Auswahl AW ermöglicht eine, dem jeweiligen Sicherheitserfordernis angepaßte Vergleichsprozedur VP, die schnell bei geringen Ansprüchen und einer geringen Anzahl von Teilabdrücken abläuft, und entsprechend langsamer bei Hochsicherheitsanwendungen geschieht.

Die Auswahl der verwendeten Teilabdrücke kann ohne Einschränkung der Sicherheit auch durch das Schreib/Lesegerät SLG erfolgen.

Die ausgewählten Teilabdrücke werden vom biometrischen Erfassungssystem BM erfaßt und mit den gespeicherten und kryptologisch geschützten Daten SPD verglichen. Ergibt der Vergleich VP eine Übereinstimmung, dann wird die eigentliche Chipkartenfunktion CF, beispielsweise eine elektronische Geldbörse oder ein Zutrittsschlüssel freigegeben.

Bei Nichtübereinstimmung erfolgen maximal zwei weitere Vergleichsvorgänge VV, wenn auch diese keine Übereinstimmung ergeben, wird die Chipkarte gesperrt SPE, wobei die Sperre zeitlich begrenzt sein kann.

Die Kartenpersonalisierung, d. h. die Speicherung bestimmter Fingerabdrücke auf einer Chipkarte geschieht wie folgt: Die "neue" Chipkarte wird vom Benutzer in das Schreib/Lesegerät eingebracht. Es ist dabei denkbar, daß nur ausgewählte Schreib/Lesegeräte beispielsweise in Banken zur Auslösung eines Personalisierungsvorganges berechtigt werden. Ein von dem Gerät ausgehender Initialisierungsimpuls veranlaßt dann die Speicher- und Vergleichslogik über die Sensormatrizen SM den/die Fingerabdrücke einzulesen und zu speichern. Danach ist keine Änderung dieser Daten mehr möglich.

Um in bestimmten Anwendungsfällen ein authorisiertes Auslesen und Verändern der Daten durch eine zentrale Stelle zu ermöglichen, kann eine kryptologisch geschützte Schnittstelle vorgesehen werden, wobei die auf der Chipkarte gespeicherten Daten entsprechend dem sogenannten RSA -Verfahren, wie es in der Zeitschrift Informationstechnik it 32 (1990), Seiten 24—32 "Algorithmen, Mechanismen und Dienste"; R. Oldenbourg Verlag beschrieben ist, mit dem "öffentlichen Teil" eines asymmetrischen Schlüsselverfahrens verschlüsselt werden.

Fig. 5 zeigt ein Identifikationssystem bei dem als biometrisches Identifikationsmerkmal die Netzhaut dient. Dabei hat der Benutzer durch ein Loch L in der Chipkarte eine Lichtquelle LQ im Schreib/Lesegerät zu blikken, so daß eine Visierlinie gebildet wird. Optische Sensoren S auf der dem Benutzer zugewandten Seite der Chipkarte erfassen dann die Struktur der Netzhaut.

Zur Erleichterung des Bedienungsvorganges umfaßt das Schreib/Lesegerät einen beweglichen Teil A, der die Chipkarte aufnimmt und an das Auge herangeführt werden kann. Der bewegliche Teil A ist mit dem Festteil B des Schreib/Lesegerätes mittels Kabel K verbunden.

Bevorzugte Anwendungsgebiete des erfindungsgemäßen Identifikationssystemes sind insbesondere die elektronische Geldbörse, also der Ersatz von Bargeld und/oder Kreditkarten, Zugangs- und Zutrittskontrollen aller Art, damit insbesondere der Ersatz von mechanischen Schlüsseln, die Personenidentifizierung und Authentifizierung, damit der Ausweisersatz, sowie der Einsatz als Datenspeicher z. B. für persönliche Daten wie die Ergebnisse von ärztlichen Untersuchungen.

Patentansprüche

1. Identifikationssystem mit elektronischer Chipkarte, mit Speichern für biometrische Identifikationsmerkmale der benutzungsberechtigten Personen, mit Sensoren zum Erfassen der biometrischen Identifikationsmerkmale und Mitteln zum Vergleich der gespeicherten und der erfaßten biometrischen Identifikationsmerkmale, **dadurch gekennzeichnet,** daß die Mittel zum Speichern (VSL), zur Erfassung (SM) und zum Vergleich (VSL) der biometrischen Identifikationsmerkmale jeweils zumindest teilweise in der Weise in die Chipkarte integriert sind, daß ein autonomer Vergleich der gespeicherten mit den erfaßten biometrischen Identifikationsmerkmale möglich ist und kein Austausch sicherheitsrelevanter Daten zwischen der elektronischen Chipkarte und den übrigen Komponenten des Identifikationssystemes erfolgt.
2. Identifikationssystem nach Anspruch 1, dadurch gekennzeichnet, daß als biometrisches Identifikationsmerkmal zumindest ein Fingerabdruck einer benutzungsberechtigten Person vorgesehen ist.
3. Identifikationssystem nach Anspruch 2, dadurch gekennzeichnet, daß die Sensoren (SM) zum Erfassen des zumindest einen Fingerabdruckes ein Transistorarray beinhalten, und daß die Transistoren so geschaltet sind, daß das thermische Abbild des zumindest einen Fingerabdruckes erfaßt wird.
4. Identifikationssystem nach Anspruch 1, dadurch gekennzeichnet, daß als biometrisches Identifikationsmerkmal die Struktur der Netzhaut vorgesehen ist.

Hierzu 2 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 196 48 767 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 26. Juni 1997

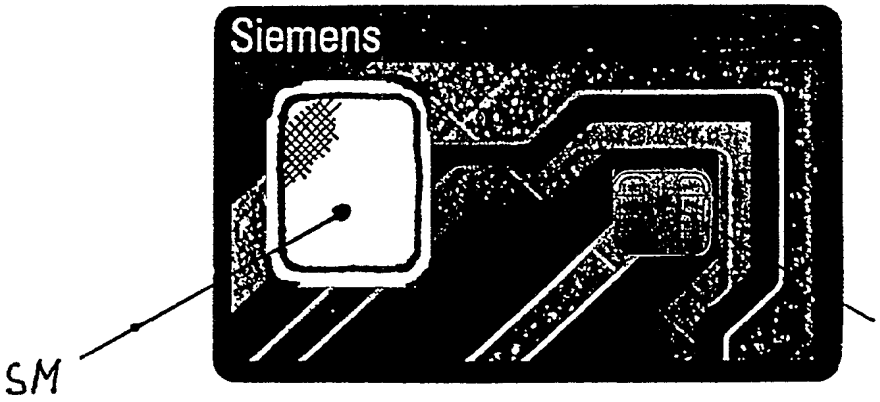


Fig.1

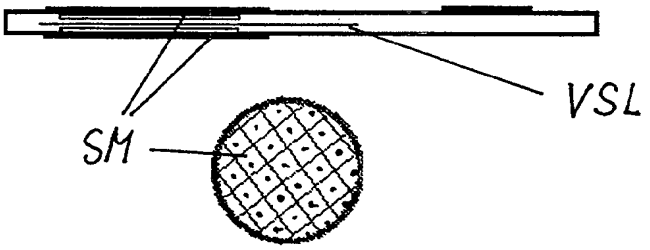


Fig.2

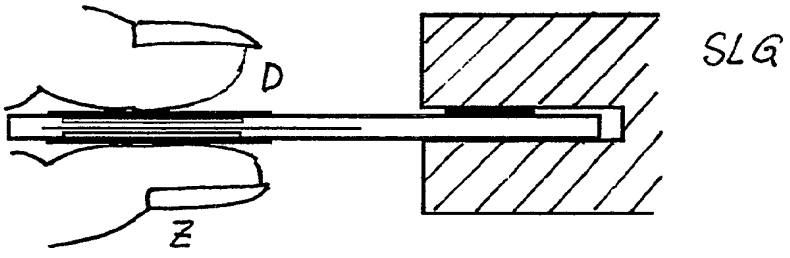


Fig. 3

Nummer: DE 196 48 767 A1
Int. Cl.[6]: G 07 C 9/00
Offenlegungstag: 26. Juni 1997

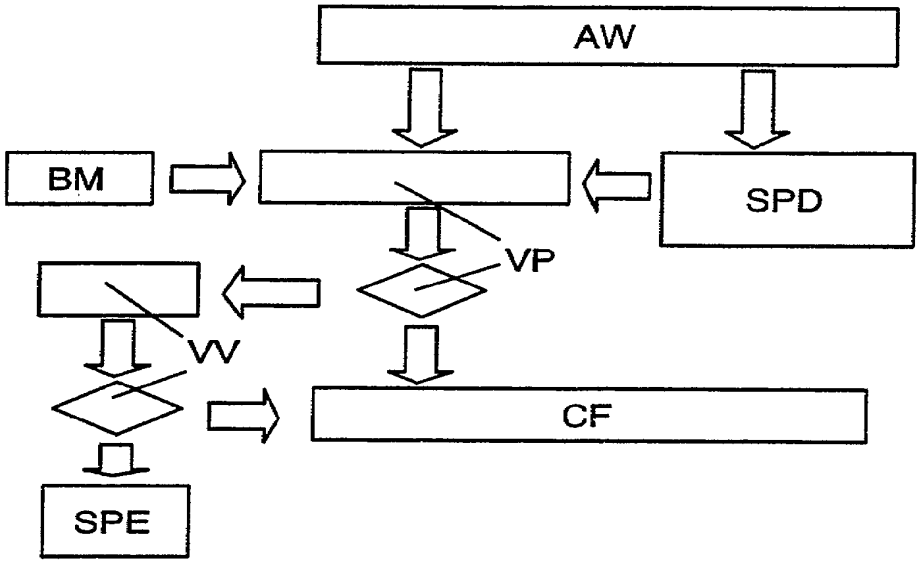


Fig.4

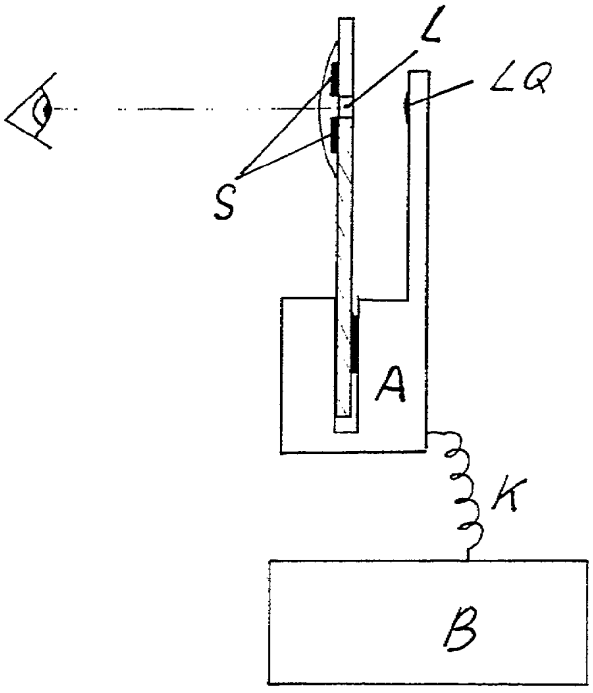


Fig.5

German Patent Application No. DE 196 48 767 A1
(Offenlegungsschrift)

FEDERAL REPUBLIC OF GERMANY
GERMAN PATENT OFFICE
PATENT APPLICATION NO. DE 196 48 767 A1

Int. Cl.[6]:	G 07 C 9/00 G 07 F 7/10 G 06 K 19/07 A 61 B 5/117
Filing No.:	196 48 767.6
Filing Date:	November 25, 1996
Publication Date:	June 26, 1997
Priority	
Date:	December 21, 1995
Country:	Austria
No.:	2084/95

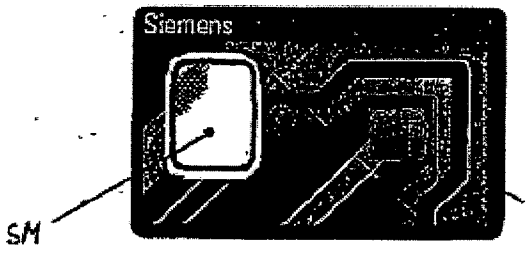
ELECTRONIC CHIP CARD IDENTIFICATION SYSTEM

Inventor:	Rudolf Rechberger Steinriegl, Austria
Applicant:	Siemens AG Österreich, Vienna, Austria
Agent:	Dr. F. Fuchs Patent Attorney 81541 Munich

Petition for examination has been submitted in accordance with § 44 of the patent law.

What is claimed is an identification system with electronic chip card, with memory (VSL) for biometric identification characteristics of the authorized persons, with sensors (SM) for detection of the biometric identification characteristics and means (VSL) for comparison of the stored and detected biometric identification characteristics in which the means for storage, for detection and for comparison of biometric identification characteristics, are each at least partially integrated into the chip card so that an autonomous comparison of the stored and detected biometric identification characteristics is possible.

With this system personal identification that is unambiguous and free of manipulation is possible without a PIN number or photo.



Description

The invention concerns an identification system with an electronic chip card [smart card], with memory for biometric identification characteristics of authorized persons, with sensors for detection of biometric identification characteristics, and means for comparison of the stored and detected biometric identification characteristics.

The spread and marketing of services in which access to protected data must be provided increasingly takes place by means of systems for electronic data processing, where electronic chip cards play an important role. For example, they are used in combination with an individual identification—the PIN number—in cash dispensing machines to verify authorization and also as an electronic wallet, to which monetary sums can be entered and then, in a cashless transaction, again deducted by the appropriate card read/write apparatus.

Through the combination of chip card and PIN number the probability of misuse is indeed reduced, but at the same time convenience for the user is also reduced, the error frequency in using the card increases and the process of authorization control is drawn out, which, for example, during primary business hours leads to considerable waiting times and lines at cash dispensing machines.

Further complicating things is also the diverse use of different chip cards for varied services in telecommunications, in access control to high security areas like research centers, or in the public health system, so that the user also has to keep in mind different PIN numbers for the use of the different chip cards.

This is why many users write down the PIN numbers and in this way considerably reduce the security of the chip card-PIN number combination.

This is why there are already systems, especially for access control, in which biometric data, for example a fingerprint, of an authorized user are stored on a chip card, and these data are compared with the fingerprint of the user at the access control point by a control apparatus,

mostly a personal computer with a connected sensor, and if the two fingerprints correspond entrance is allowed.

In addition, a system for fingerprint identification in which a fingerprint sensor is integrated into a chip card is known from WO 94/25938.

It is disadvantageous with the said systems in particular that data relevant to security—the information on the fingerprint—are transferred from the chip card to a control system and thus can be stolen.

The invention therefore is based on the task of specifying an identification system that satisfies the highest security requirements.

In accordance with the invention this takes place with an identification system of the kind mentioned above, in which the means for storage (VSL), for detection (SM), and for comparison (VSL) of the biometric identification characteristics are each at least partially integrated into the chip card, in which an autonomous comparison of the stored and detected biometric identification characteristics is possible and no exchange of data relevant to security takes place between the electronic chip card and the other components of the identification system.

Personal characteristics that are suitable for identification are, for example, the pattern of the blood vessels of the retina, the structure of the iris, the length and shape of the fingers, the face, the voice, or even fingerprints. The possibilities of identifying persons by means of these characteristics are described, for example, in IEEE Spectrum, February, 1994, "It had to be you." The fingerprints here are probably the best researched and thus the most reliable characteristics, and reliability can be increased even further by checking more than one fingerprint. The fingerprints can also be identified in a manner that is convenient for the user, while the pattern of the retina, for example, can be detected only by a procedure that is inconvenient for the person being identified and therefore can only be used in those instances in which this effect is not important or even desirable.

It is advantageous if the sensors for detection of the minimum of one fingerprint consist of a transistor array and the transistors are connected so that the thermal image of the minimum of one fingerprint is detected. Transistors are, as is known, characterized by high capacity for integration and a sensor designed in this way therefore can be produced with small measurements, especially low thickness.

The invention is illustrated in more detail by means of figures. Here, as examples:

Figure 1 shows a chip card designed in accordance with the invention,

Figure 2 shows a cross section through the chip card as in Figure 1,

Figure 3 shows the use of a chip card as in Figure 1 and Figure 2,

Figure 4 shows a block diagram of the identification testing process, and

Figure 5 shows the structure of an identification system in which the retina is scanned as the biometric identification characteristic.

The core of the identification system in accordance with the invention is the chip card shown in Figures 1, 2 and 3. Besides a storage and comparison logic VSL, it contains two sensor matrices SM formed from individual transistors, with which the fingerprints from the thumb D and index finger Z are detected. In order to make the use of the card easier, it is also possible to eliminate one sensor matrix and the detection of the print of the index finger.

Power is supplied to the chip card via a read/write apparatus SLG, to which there is also a data connection via which the data exchange necessary for the intended use takes place. If the chip card is used as an electronic wallet, this means entry or deduction of electronic sums of money.

For the identification process relevant data such as the stored fingerprint patterns are not exchanged via this data connection, so that said data cannot be stolen even via an appropriately prepared read/write apparatus.

The sensor matrices SM consist of an array of transistors that are connected so that they serve as temperature sensors. Here the ridges and valleys of the fingerprint are detected via temperature differences when a finger is placed on the sensor matrix.

The course of an identification process is illustrated by means of Figure 4:

In the embodiment example the fingerprint is broken down into a certain number of significant partial prints. Each identification process makes use of only a part of the fingerprint, which is randomly or pseudo-randomly selected. This selection AW enables a comparison procedure VP that is matched to the relevant security requirement, which is quick if security demands are low and a small number of partial prints is used, and is correspondingly slower in high security applications.

The selection of the partial prints that are used can also take place via the read/write apparatus SLG without limiting security.

The selected partial prints are detected by the biometric detection system BM and compared with the stored and cryptologically protected data SPD. If the comparison VP yields a correspondence, then the actual chip card function CF, for example, an electronic wallet or entrance key, is enabled.

If there is no correspondence, then a maximum of two additional comparison processes VV takes place, and if these also do not provide correspondence, the chip card becomes blocked SPE, where the block can be limited in time.

Personalization of the card, i.e., storage of specific fingerprints on the chip card, takes place as follows: The "new" chip card is inserted by the user into the read/write apparatus. Here it is conceivable that only selected read/write apparatuses, for example in banks, are authorized

to initiate a personalization operation. An initialization impulse coming from the apparatus then permits the memory and comparison logic to read the fingerprint or fingerprints via the sensor matrices SM and to store them. After that no change of said data is possible.

In order to allow authorized readout and modification of the data by a central site in some cases, a cryptologically protected interface can be provided, where data stored on the chip card can be encrypted with the "open part" of an asymmetric key process in accordance with the RSA method, as described in the journal Informationstechnik it 32 (1990), pp. 24-32 "Algorithms, mechanisms and services," R. Oldenbourg Publishers.

Figure 5 shows an identification system in which the retina serves as biometric identification characteristic. Here the user looks through a hole L in the chip card at a light source LQ in the read/write apparatus so that a line of sight is formed. Optical sensors S on the side of the chip card turned toward the user then detect the structure of the retina.

To facilitate the operation the read/write apparatus has a movable part A that holds the chip card and can moved up to the eye. The movable part A is connected to the fixed part B of the read/write apparatus by means of cable K.

Preferred areas for use of the identification system in accordance with the invention are in particular the electronic wallet, thus the replacement of cash and/or credit cards, entry and access control of all kinds, thus in particular the replacement of mechanical keys, personnel identification and authentification, thus the replacement of identification cards, and as data storage, for example, for the personal data such as the results of medical tests.

Claims

1. An identification system with an electronic chip card, with memory for biometric identification characteristics of authorized persons, with sensors for detection of the biometric identification characteristics, and means for comparison of the stored and detected biometric identification characteristics, characterized by the fact that the means for storage (VSL), for detection (SM), and for comparison (VSL) of the biometric identification characteristics are each at least partially integrated into the chip card so that autonomous comparison of the stored and detected biometric identification characteristics is possible and no exchange of data relevant to security takes place between the electronic chip card and the other components of the identification system.

2. An identification system as in Claim 1, characterized by the fact that at least one fingerprint of an authorized person is specified as the biometric identification characteristic.

3. An identification system as in Claim 2, characterized by the fact that the sensors (SM) for detection of the minimum of one fingerprint consist of a transistor array and the transistors are connected so that the thermal image of the minimum of one fingerprint is detected.

4. An identification system as in Claim 1, characterized by the fact that the structure of the retina is specified as biometric identification characteristic.

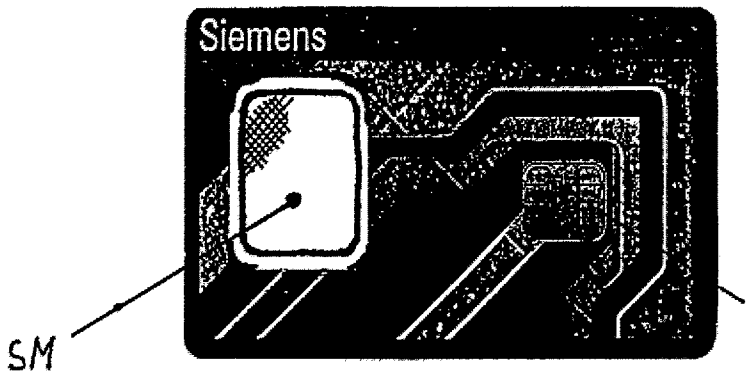


Fig.1

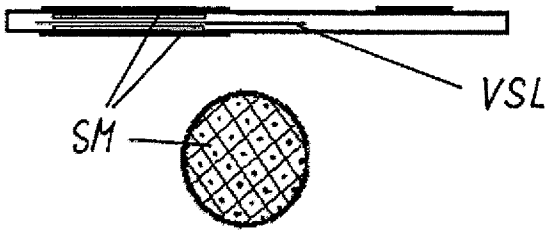


Fig.2

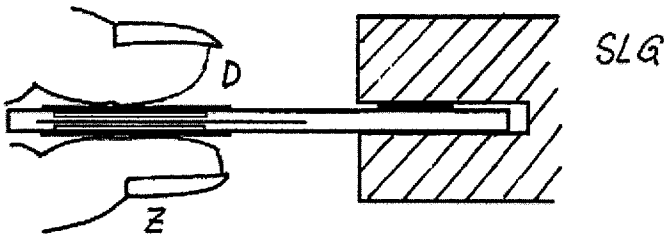


Fig. 3

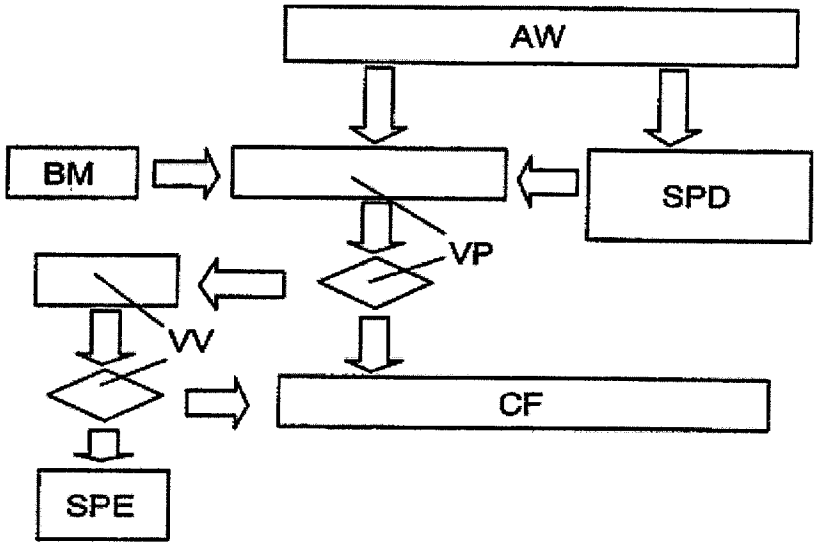


Fig.4

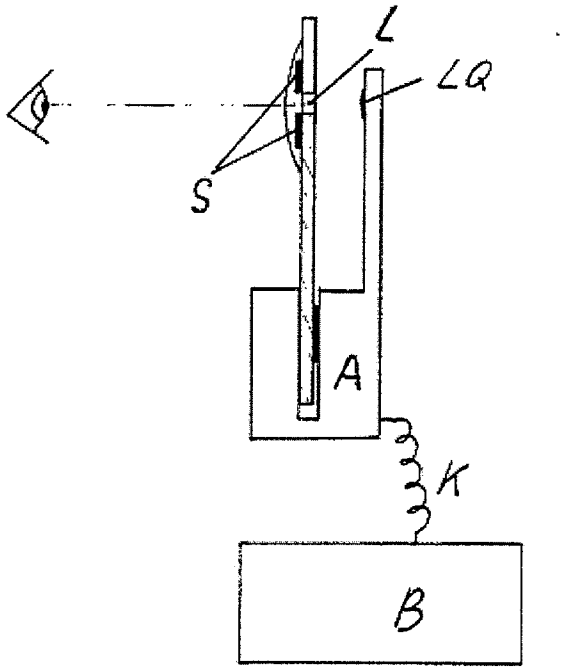


Fig.5